User Manual for the NETGEAR RangeMax™ Wireless PCI Adapter WPN311

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

Version v1.0
February 2005

Technical Support

Please refer to the support information card that shipped with your product. By registering your product at *http://www.netgear.com/register*, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

E-mail: support@netgear.com

Web site: *http://www.netgear.com*

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

© 2005 NETGEAR, Inc. NETGEAR, the NETGEAR logo, The Gear Guy and Everybody's Connecting are trademarks or registered trademarks of NETGEAR, Inc. in the United States and/or other countries. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

February 2005

Certificate of the Manufacturer/Importer

It is hereby certified that the Model WPN311Wireless PCI Adapter has been suppressed in accordance with the conditions set out in the BMPT- AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

FCC Guidelines for Human Exposure

In order to comply with RF exposure limits established in the ANSI C95.1 standards, the user is advised to maintain a distance of at least 1 inch (2.5 cm) from the antenna of this device while it is in use.

FCC Electronic Emission Notices

This device complies with part 15 of the FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause harmful interference
2. This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Statement

NETGEAR RangeMax™ Wireless PCI Adapter WPN311

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

FCC ID: PY3WG311TV3

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

Operation of this equipment in a residential area may cause harmful interference, in which case the user will be required to correct the interference at his own expense.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Export Restrictions

This product or software contains encryption code which may not be exported or transferred from the US or Canada without an approved US Department of Commerce export license.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Model WPN311 Wireless PCI Adapter) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Canada ID: 4054A-WG311TV3

Product and Publication Details

Model Number:	WPN311
Publication Date:	February 2005
Product Family:	wireless access point
Product Name:	NETGEAR RangeMax™ Wireless PCI Adapter WPN311
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10074-01

Contents

Chapter 1
About This Manual

Audience, Scope, Conventions 1-1
How to Print this Manual 1-2

Chapter 2
Introduction

About the NETGEAR RangeMax™ Wireless PCI Adapter WPN311 2-1
Key Features and Related NETGEAR Products 2-1
What's in the Box? 2-2
A Road Map for 'How to Get There From Here' 2-3

Chapter 3
Basic Setup

What You Will Need Before You Begin 3-1
Verify System Requirements 3-1
Observe Location and Range Guidelines 3-2
Two Basic Operating Modes 3-2
WPN311 Default Wireless Configuration Settings 3-2
Basic Installation Instructions 3-3
For Windows XP Users Installing a WPN311 3-4
For Windows 2000 & 98SE/Me Users Installing a WPN311 3-8
WPN311 Wireless Connection Indicators 3-11
Interpreting System Tray Icon Colors 3-12
Basic Troubleshooting Tips 3-12
About Page 3-13

Chapter 4
Configuration

Understanding the Configuration Options 4-1
Using Configuration Profiles 4-1
Networks Page 4-2
Connecting to an Access Point in Infrastructure Mode 4-3
How to Configure an Infrastructure Mode Profile 4-3

Connecting to Another PC in Ad-Hoc Mode 4-5
How to Configure an Ad-Hoc Mode Profile 4-5
Enabling Wireless Security Features 4-8
Identifying the Wireless Security Settings 4-9
How to Configure WEP Encryption Security 4-10
How to Configure WPA-PSK Encryption Security 4-11
Statistics Page 4-12
Advanced Settings Page 4-13

Chapter 5
Troubleshooting

Frequently Asked Questions 5-1
General Questions 5-1
Wi-Fi Protected Access (WPA) Questions 5-3

Appendix A
Technical Specifications A1

Appendix B
Wireless Networking Basics

Wireless Networking Overview B-1
Infrastructure Mode B-1
Ad-Hoc Mode (Peer-to-Peer Workgroup) B-2
Network Name: Extended Service Set Identification (ESSID) B-2
Authentication and WEP B-2
802.11 Authentication B-3
Open System Authentication B-3
Shared Key Authentication B-4
Overview of WEP Parameters B-5
Key Size B-6
WEP Configuration Options B-6
Wireless Channels B-7
WPA Wireless Security B-8
How Does WPA Compare to WEP? B-9
How Does WPA Compare to IEEE 802.11i? B-10
What are the Key Features of WPA Security? B-10
Is WPA Perfect? B-16
Product Support for WPA B-16

Appendix C
Preparing Your PCs for Network Access

Preparing Your Computers for TCP/IP Networking C-1
Configuring Windows 98SE and Me for TCP/IP Networking C-1
Install or Verify Windows Networking Components C-1
Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 98SE and Me C-3
Selecting the Internet Access Method C-5
Verifying TCP/IP Properties C-5
Configuring Windows 2000 or XP for TCP/IP Networking C-6
Install or Verify Windows Networking Components C-6
DHCP Configuration of TCP/IP in Windows XP or 2000 ..... C-7
DHCP Configuration of TCP/IP in Windows XP C-7
DHCP Configuration of TCP/IP in Windows 2000 ..... C-9
Verifying TCP/IP Properties for Windows XP or 2000 ..... C-11

Glossary

List of Glossary Terms G-1

Index

Chapter 1
About This Manual

Audience, Scope, Conventions

This manual assumes that the reader has basic to intermediate computer and Internet skills. However, tutorial information is provided in the Appendices, on the *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD*, and on the NETGEAR Web site.

This manual uses the following typographical conventions:

Table 1-1. Typographical conventions

italics	Emphasis.
bold	User input.
SMALL CAPS	File and directory names.

This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

This manual is written according to these specifications:

Table 1-2. Manual Specifications

Product Version	NETGEAR RangeMax™ Wireless PCI Adapter WPN311
Manual Part Number	202-10075-01
Manual Publication Date	February 2005

Note: Product updates are available on the NETGEAR Web site at *http://www.netgear.com/support/main.asp*.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Chapter**. Use the PDF of This Chapter link at the top right of any page.
  - Click "PDF of This Chapter" link at the top right of any page in the chapter you want to print. A new browser window opens showing the PDF version of the chapter you were viewing.
  - Click the print icon in the upper left of the window.
  - **Tip**: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.
- **Printing the Full Manual**. Use the PDF button in the toolbar at the top right of the browser window.
  - Click PDF button. A new browser window opens showing the PDF version of the chapter you were viewing.
  - Click the print icon in the upper left of the window.
  - **Tip**: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 2
Introduction

This chapter introduces the features, package contents, and appearance of the NETGEAR RangeMax™ Wireless PCI Adapter WPN311.

About the NETGEAR RangeMax™ Wireless PCI Adapter WPN311

The NETGEAR RangeMax™ Wireless PCI Adapter WPN311 gives you flexibility to install the PC in the most convenient location available. The WPN311 frees you from traditional Ethernet wiring that is limited by cabling requirements.

Its auto-sensing capability allows high packet transfer up to 108 Mbps for maximum throughput or dynamic range shifting to lower speeds due to distance or operating limitations in an environment with a lot of electromagnetic interference.

The WPN311 Wireless PCI Adapter provides reliable, standards-based 802.11b 11 Mbps Wireless Local Area Network (WLAN) connectivity that is protected with industry-standard security. In addition, it offers the faster speeds of the 802.11g standard. The WPN311 works with Windows 98SE, Me, 2000, and XP operating systems.

Key Features and Related NETGEAR Products

The WPN311 Wireless PCI Adapter provides the following features:

- Reliable IEEE 802.11b/g standards-based wireless technology.
- Supports roaming between access points when configured in Infrastructure mode.
- 108 Mbps high speed data transfer. Wireless nodes negotiate to operate in the optimal data transfer rate. In a noisy environment or when the distance between the wireless nodes is far, the wireless nodes automatically fall back to operate at lower transfer rates.
- High level of data encryption using128-bit Shared Key WEP data encryption method. Lower level of data encryption or no data encryption is available to simplify your network setup or to improve the data transfer rate.

The following NETGEAR products can be configured to communicate with the WPN311 Wireless PCI Adapter:

- WPN824 RangeMax™ Wireless Router
- WGT634U 108 Mbps Wireless Media Router
- WGT624 108 Mbps Wireless Firewall Router
- WG602 54 Mbps Wireless Access Point
- WGR614 54 Mbps Cable/DSL Wireless Router
- WGR511 54 Mbps Wireless PC Card
- MA111 802.11b Wireless USB Adapter
- ME103 802.11b ProSafe Wireless Access Point
- MA311 802.11b Wireless PCI Adapter
- MR814 802.11b Wireless Cable/DSL Routers
- MA521 802.11b Wireless Compact Flash Card

What's in the Box?

The product package should contain the following items:

- NETGEAR RangeMax™ Wireless PCI Adapter WPN311
- User Manual for the NETGEAR RangeMax™ Wireless PCI Adapter WPN311
- *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD*, including:
  - — Driver Software
  - — Wireless Assistant
  - — Installation Guide
- Warranty card
- Support information card

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

A Road Map for 'How to Get There From Here'

The introduction and adoption of any new technology can be a difficult process. Wireless technology has removed one of the barriers to networking—running wires. It allows more people to try networking, while at the same time exposes them to the inherent complexity of networking. General networking concepts, set up, and maintenance can be difficult to understand. In addition, wireless technology adds issues such as range, interference, signal quality, and security to the picture.

To help overcome potential barriers to successfully using wireless networks, the table below identifies how to accomplish such things as connecting to a wireless network, assuring appropriate security measures are taken, browsing the Internet through your wireless connection, exchanging files with other computers and using printers in the combined wireless and wired network.

Table 2-1. A Road Map for How to Get There From Here

If I Want To ... ?	What Do I Do?	What's Needed?	How Do I?
Connect to a wireless network	1. Identify the wireless network name (SSID) and, if used, the wireless security settings. 2. Set up the NETGEAR RangeMax™ Wireless PCI Adapter WPN311 with the settings from step 1.	1. A wireless network 2. A desktop PC within the operating range of the wireless network. For guidelines about the range of 802.11b/g wireless networks, please see "Observe Location and Range Guidelines" on page 3-2.	To set up the WPN311, see Chapter 3, "Basic Setup" and follow the instructions provided. To learn about wireless networking technology, see Appendix B, "Wireless Networking Basics" for a general introduction.

Table 2-1. A Road Map for How to Get There From Here

If I Want To ... ?	What Do I Do?	What's Needed?	How Do I?
Protect my wireless connection from snooping, hacking, or information theft.	1. Assure that the wireless network has security features enabled. 2. Configure my WPN311 with the security settings of the wireless network. 3. Use Windows security features.	1. A wireless network with authentication and WEP encryption enabled. 2. Wireless networking equipment that supports WEP encryption, such as the WPN311 and all NETGEAR wireless networking products.	To learn about wireless networking security, see "Authentication and WEP" on page B-2. To use wireless security features, please see "Enabling Wireless Security Features" on page 4-8 and configure your WPN311 accordingly.
Note: Secure Internet sites such as banks and online merchants use encryption security built into browsers like Internet Explorer and Netscape. Any wireless networking security features you might implement are in addition to those already in place on secure Internet sites.			
Connect to the Internet over my wireless network.	1. Activate my wireless link and verify my network connection. 2. Open an Internet browser such as Internet Explorer or Netscape Navigator.	1. An active Internet connection like those from cable or DSL service providers. 2. A wireless network connected to the cable or DSL Internet service through a cable/DSL router as illustrated in "Connecting to an Access Point in Infrastructure Mode" on page 4-3. 3. TCP/IP Internet networking software installed and configured on my PC according to the requirements of the Internet service provider 4. A browser like Internet Explorer or Netscape Navigator.	To configure your WPN311 in Infrastructure Mode, see "Basic Installation Instructions" on page 3-3, and locate the section for your version of Windows. For assistance with configuring the TCP/IP Internet software on a PC, see "Preparing Your Computers for TCP/IP Networking" on page C-1 or refer to the PC Networking Tutorial on the *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD* and the Help information provided in the Windows system you are using. .

Table 2-1. A Road Map for How to Get There From Here

If I Want To ... ?	What Do I Do?	What's Needed?	How Do I?
Exchange files between a wirelessly connected notebook computer and other computers in a my combined wireless and wired network.	1. Use the Windows Network Neighborhood feature to browse for computers in the combined wireless and wired network. 2. Browse the hard drive of the target computer in the network in order to locate the directory or files you want to work with. 3. Use the Windows Explorer copy and paste functions to exchange files between the computers.	1. The desktop computer I am using to connect to the wireless network needs to be configured with the Windows Client and File and Print Sharing. 2. The desktop computer I am using to connect to the wireless network needs to be configured with the same Windows Workgroup or Domain settings as the other Windows computers in the combined wireless and wired network. 3. Any Windows networking security access rights such as login user name/ password that have been assigned in the Windows network or for sharing particular files must be provided when Windows prompts for such information. 4. If so-called Windows 'peer' Workgroup networking is being used, the drive, file system directory, or file need to be enabled for sharing.	For assistance with Windows networking software, see Appendix C, "Preparing Your PCs for Network Access" for configuration scenarios or refer to the Help system included with your version of Windows. Windows Domain settings are usually managed by corporate computer support groups. Windows Workgroup settings are commonly managed by individuals who want to set up small networks in their homes, or small offices. For assistance with setting up Windows networking, refer to the PC Networking Tutorial on the *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD* and the Help information provided in the Windows system you are using.

Table 2-1. A Road Map for How to Get There From Here

If I Want To ... ?	What Do I Do?	What's Needed?	How Do I?
Use printers in a combined wireless and wired network.	1. Use the Windows Printers and Fax features to locate available printers in the combined wireless and wired network. 2. Use the Windows Add a Printer wizard to add access to a network printer from the PC you are using to wirelessly connect to the network. 3. From the File menu of an application such as Microsoft Word, use the Print Setup feature to direct your print output to the printer in the network.	1. The desktop computer I am using to connect to the wireless network needs to be configured with the Windows Client and File and Print Sharing. 2. The desktop computer I am using to connect to the wireless network needs to be configured with the same Windows Workgroup or Domain settings as the other Windows computers in the combined wireless and wired network. 3. Any Windows networking security access rights such as login user name/ password that have been assigned in the Windows network must be provided when Windows prompts for such information. 4. If so-called Windows 'peer' networking is being used, the printer needs to be enabled for sharing.	Windows Domain settings are usually managed by corporate computer support groups. Windows Workgroup settings are commonly managed by individuals who want to set up small networks in their homes, or small offices. For assistance with setting up Windows networking, refer to the PC Networking Tutorial on the *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD* and the Help information provided in the Windows system you are using. For assistance with setting up printers in Windows, refer to the Help and Support information that comes with the version of the Windows operating systems you are using.

Chapter 3
Basic Setup

This section describes how to install your NETGEAR RangeMax™ Wireless PCI Adapter WPN311 and set up basic wireless connectivity on your Wireless Local Area Network (WLAN). Advanced wireless network configuration is covered in Chapter 4, “Configuration” in this manual.

Note: Indoors, computers can easily connect to 802.11 wireless networks at distances of several hundred feet. Because walls do not always block wireless signals, others from outside your immediate area could access your network. It is important to take appropriate steps to secure your network from unauthorized access. The NETGEAR RangeMax™ Wireless PCI Adapter WPN311 provides highly effective security features which are covered in “Enabling Wireless Security Features” on page 4-8. Deploy the security features appropriate to your needs.

What You Will Need Before You Begin

You need to verify that your computer meets the minimum system requirements and identify the wireless network configuration settings of the WLAN where you will connect before you can configure your wireless pc adapter and connect.

Verify System Requirements

Before installing the NETGEAR RangeMax™ Wireless PCI Adapter WPN311, please make sure that these minimum requirements have been met:

- Pentium® III class computer with an available PCI slot
- CD drive
- 20 Mbytes of free hard disk space
- Some versions of Windows may ask for the original Windows operating system installation files to complete the installation of the WPN311 driver software

Observe Location and Range Guidelines

Computers can connect over 802.11g wireless networks indoors at a range which varies significantly based on the physical location of the computer with the NETGEAR RangeMax™ Wireless PCI Adapter WPN311. For best results, avoid potential sources of interference, such as:

- Large metal surfaces
- Microwaves
- 2.4 GHz Cordless phones

In general, 802.11g wireless devices can communicate through walls. However, if the walls are constructed with concrete, or have metal, or metal mesh, the 802.11g effective range will decrease if such materials are between the devices.

Two Basic Operating Modes

The WPN311 Wireless PCI Adapter, like all 802.11b/g adapters, can operate in the following two basic modes:

- **Infrastructure Mode:** An 802.11 networking framework in which devices and computers communicate with each other by first going through an access point (AP). For example, this mode is used when computers in a house connect to an AP that is attached to a router which lets multiple computers share a single Cable or DSL broadband Internet connection.
- **Ad-Hoc Mode:** An 802.11 networking framework in which devices or computers communicate directly with each other, without the use of an access point. For example, Ad-Hoc Mode is used when two Windows computers are configured with file and print sharing enabled and you want to exchange files directly between them.

Both of these configuration options are available with the WPN311 Wireless PCI Adapter. Infrastructure configuration procedures for basic network connectivity are covered below. Advanced infrastructure configuration procedures and ad-hoc configuration are covered in Chapter 4, “Configuration” of this manual.

WPN311 Default Wireless Configuration Settings

If this is a new wireless network installation, use the factory default settings to set up the network and verify wireless connectivity. If this is an addition to an existing wireless network, you will need to identify the wireless configuration and security parameters already defined.

Your NETGEAR RangeMax™ Wireless PCI Adapter WPN311 factory default basic settings are:

- Network Name Service Set Identification (SSID): **ANY** — a special name which indicates the first available network will be used

  Note: In order for the WPN311 Wireless PCI Adapter to communicate with a wireless access point or wireless adapter, all devices must be configured with the same wireless network name (SSID).

- Network Mode (Infrastructure or Ad-Hoc): **Infrastructure**
- Data security WEP encryption: **Disabled**

The section below provides instructions for setting up the NETGEAR RangeMax™ Wireless PCI Adapter WPN311 for basic wireless connectivity to an access point. The procedures provide step-by-step installation instructions for Windows PCs. Use the procedure that corresponds to the version of Windows you are using.

Basic Installation Instructions

Use the procedure below that corresponds to the version of Windows you are using.

For Windows XP Users Installing a WPN311

1

Install the WPN311 software.

a. Power on your computer, let the operating system boot up completely, and log in as needed.

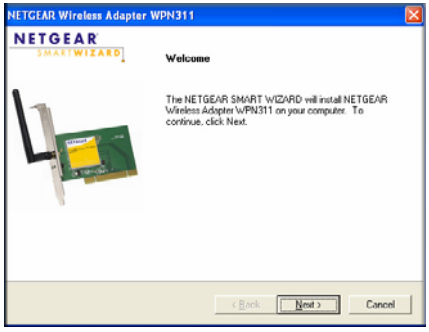
b. Insert the *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD* into your CD drive. The CD main page shown at the right loads.

c. Click the "Install Driver & Utility" link.

d. Follow the Smart Wizard - Install Assistant steps, and click Finish when done to restart your computer.

WPN311 Resource CD main page

Note: If this page does not automatically appear, browse the root of the CD and double-click on `autorun.exe` to display this page.


NETGEAR Wireless Adapter WPN311
NETGEAR
SMARTWIZARD
Welcome
The NETGEAR SMART WIZARD will install NETGEAR Wireless Adapter WPN311 on your computer. To continue, click Next.
< Back
Next >
Cancel

Smart Wizard - Install Assistant

Note: If a Windows XP Certification warning appears, click **Continue Anyway** to proceed.

2

Install the NETGEAR RangeMax™ Wireless PCI Adapter WPN311.

a. Shut down the PC and remove the power cord. Insert the WPN311 Wireless PCI Adapter into an available PCI slot.

   Connect the antenna to the adapter and position the antenna to the up position. Reconnect the power cord and reboot the computer.

b. The Found New Hardware Wizard displays. Click **Next** and follow the prompts to proceed**.**

c. When prompted, choose the country where you are located from the list.

d. You also will be prompted to enable the NETGEAR Smart Wireless Settings Utility configuration utility.

e. Click **Yes** to accept this option.

   If you choose No, you must read the Windows XP documentation to learn how to use the Windows XP wireless network configuration utility.

f. After the installation completes, click **Finish** to close the wizard.

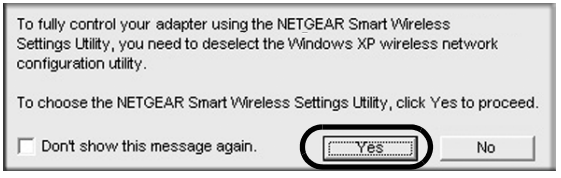
You should see the WPN311 system tray icon on the lower right portion of the Windows task bar.

Windows XP displays a Wireless Network Connection message.

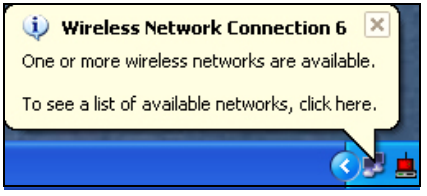
Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).
Read our privacy policy
Can Windows connect to Windows Update to search for software?
Yes, this time only
Yes, now and every time I connect a device
No, not this time
Click Next to continue.
< Back
Next >
Cancel

Found New Hardware Wizard

Note: If you are prompted with a Windows XP Logo Testing message, click **Continue Anyway**.


To fully control your adapter using the NETGEAR Smart Wireless Settings Utility, you need to deselect the Windows XP wireless network configuration utility.
To choose the NETGEAR Smart Wireless Settings Utility, click Yes to proceed.
Don't show this message again.
Yes
No

WPN311 System Tray Icon


Wireless Network Connection 6
One or more wireless networks are available.
To see a list of available networks, click here.

Windows XP Network Connection Alert

3

Configure your WPN311 and save the Profile.

a. Click the system tray icon to open the WPN311 Smart Wizard Wireless Assistant.

   The Settings page opens.

b. Change the Network Name SSID to match your network.

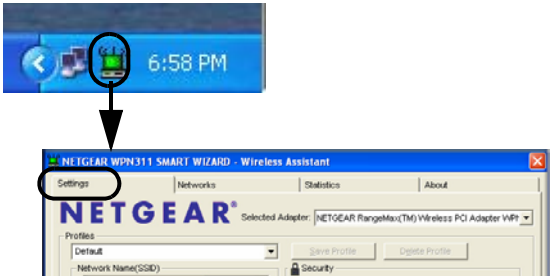
   Tip: Instead of typing in the SSID, you can use the Network tab to view the available wireless networks. Double-click on the desired network.

c. Click **Apply** to activate the connection.

d. Enter a name for your profile and click Save Profile to store the current settings.

   Tip: If you use your notebook PC to connect to a wireless network at work and at home, create profiles called *work* and *home*.

   Note: This procedure assumes your wireless network is not using security. If your wireless network uses WEP or WPA-PSK, set up your WPN311 accordingly. To view the wireless security settings help, click the Help button.



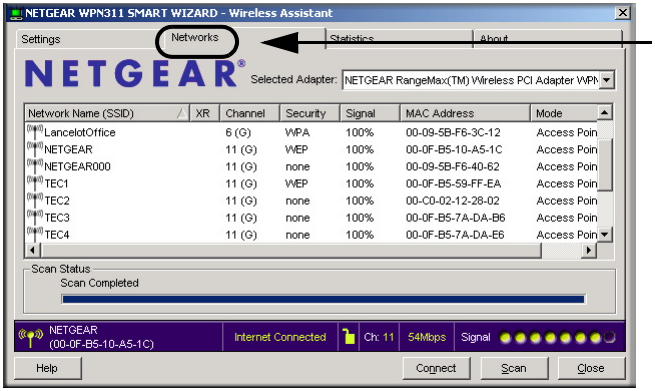
WPN311 Wireless Assistant Settings Page

Note: The NETGEAR default settings are **Infrastructure mode**, with **ANY** for the wireless network name SSID, and WEP disabled.

4

Verify wireless connectivity to your network.

a. Click the WPN311 icon in the Windows system tray to open the Smart Wizard Installation Assistant.



Note: You can use the Networks tab to verify the availability of wireless networks and their SSIDs.

For more information, see "Understanding the Configuration Options" on page 4-1.

b. Verify connectivity to the Internet or network resources.

Note: If you are unable to connect, see "Basic Troubleshooting Tips" on page 3-12.

For Windows 2000 & 98SE/Me Users Installing a WPN311

1

Install the WPN311 software.

Note: Windows 2000 may require you to be logged on with administrator rights.

a. Power on your computer, let the operating system boot up completely, and log in as needed.

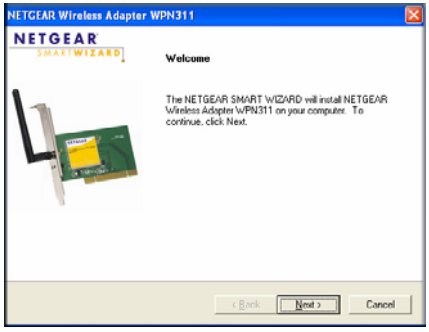
b. Insert the Resource CD for the WPN311 into your CD drive. The CD main page shown at the right will load.

c. Click the “Install Driver & Utility” link.

d. Follow the Smart Wizard - Install Assistant steps, and click Finish when done to restart your computer.

Note: If you are prompted to restart your computer, choose instead to shut it down. This will let you install the WPN311 before restarting. Windows will find the new hardware and can use the software you installed.

WPN311 Resource CD


NETGEAR Wireless Adapter WPN311
NETGEAR
SMARTWIZARD
Welcome
The NETGEAR SMART WIZARD will install NETGEAR Wireless Adapter WPN311 on your computer. To continue, click Next.
< Back
Next >
Cancel

Smart Wizard - Install Assistant

2

Install the NETGEAR RangeMax™ Wireless PCI Adapter WPN311.

a. Shut down the PC and remove the power cord. Insert the WPN311 Wireless PCI Adapter into an available PCI slot.

b. Reconnect the power cord and reboot the computer. After a short delay, the Found New Hardware Wizard displays.

c. You will be prompted to choose the country where you are located. Select your location from the list.

d. Click **Next** and follow the prompts to proceed**.** After the installation completes, click **Finish** to close the wizard.

You should see the WPN311 system tray icon on the lower right portion of the Windows task bar.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).
Read our privacy policy
Can Windows connect to Windows Update to search for software?
Yes, this time only
Yes, now and every time I connect a device
No, not this time
Click Next to continue.
< Back
Next >
Cancel

Found New Hardware Wizard

Note: If Windows displays a Digital Signature Not Found warning, click **Yes** to continue.

WPN311 System Tray Icon

3

Configure your WPN311 and save the Profile.

a. Click the system tray icon to open the WPN311 Smart Wizard Wireless Assistant.

   The Settings page opens.

b. Change the Network Name SSID to match your network.

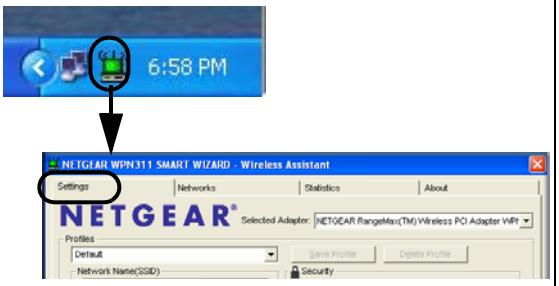
   Tip: Instead of typing in the SSID, you can use the Network tab to view the available wireless networks. Double-click on the desired network.

c. Click **Apply** to activate the connection.

d. Enter a name for your profile and click the Save Profile button to store the current settings.

   Tip: If you use your notebook PC to connect to a wireless network at work and at home, create profiles called *work* and *home*.

   Note: This procedure assumes you are connecting to a wireless network which is not using WEP security. If your network includes WEP settings, enter the security information in the Security section. For help with these steps, see "Enabling Wireless Security Features" on page 4-8.



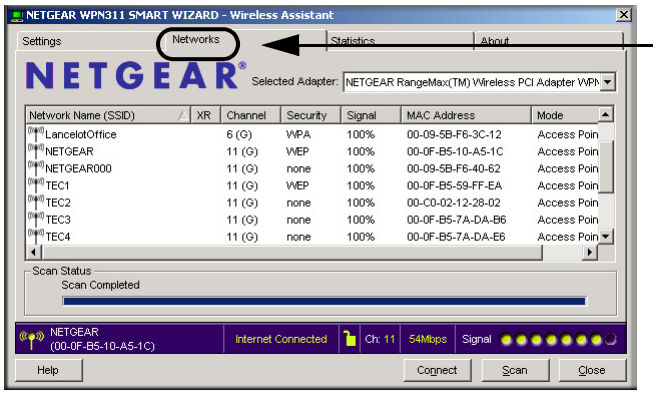
WPN311 system tray icon

Note: The NETGEAR default settings are **Infrastructure mode**, with **ANY** for the wireless network name SSID, and WEP disabled.

4

Verify wireless connectivity to your network.

a. Verify that your connection information matches your wireless network.



Note: You can use the Networks tab to verify the availability of wireless networks and their SSIDs.

For more information, see "Understanding the Configuration Options" on page 4-1.

b. Verify connectivity to the Internet or network resources.

Note: If you are unable to connect, see "Basic Troubleshooting Tips" on page 3-12.

WPN311 Wireless Connection Indicators

The NETGEAR RangeMax™ Wireless PCI Adapter WPN311 SysTray icon, which is on the System Tray portion of the taskbar in the Microsoft Windows desktop, is an indicator that gives you feedback on the status of your wireless connection. The color of the SysTray icon indicates the status of the connection.

Interpreting System Tray Icon Colors

The System Tray (SysTray) resides on one end of the taskbar in the Microsoft Windows desktop.

Color	Condition	Description
Red	The wireless PCI Adapter has no connection to any other wireless node.	The wireless PCI Adapter is not able to link to any other wireless node or the link is lost. Check your configuration or try moving to a location where the wireless signal quality is better.
Yellow	The wireless PCI Adapter has a connection with another wireless node.	The wireless link is weak. You may deed to move to a better spot, such as closer to the wireless access point. Also, look for possible interference such as a 2.4 GHz cordless phone or large metal surface.
Green	The wireless PCI Adapter has a connection with another wireless node.	The wireless PCI Adapter has established good communication with an access point and the signal quality is strong.

Basic Troubleshooting Tips

If you have problems connecting to your wireless network, try the tips below. If this does not solve the problem, see “Frequently Asked Questions” on page 5-1.

Symptom	Cause	Solution
I can connect to an access point, but I cannot connect to other computers on the network or the Internet.	This could be a physical layer problem or a network configuration problem.	Check to make sure that the access point is physically connected to the Ethernet network. Make sure that the IP addresses and the Windows networking parameters are all configured correctly. Restart the cable or DSL modem, router, access point, and notebook PC.

Also, for problems with accessing network resources, the Windows software might not be installed and configured properly on your computers. Please refer to Appendix C, “Preparing Your PCs for Network Access” of the Reference Manual on the *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD*.

About Page

The About page displays important information about the NETGEAR RangeMax™ Wireless PCI Adapter WPN311.

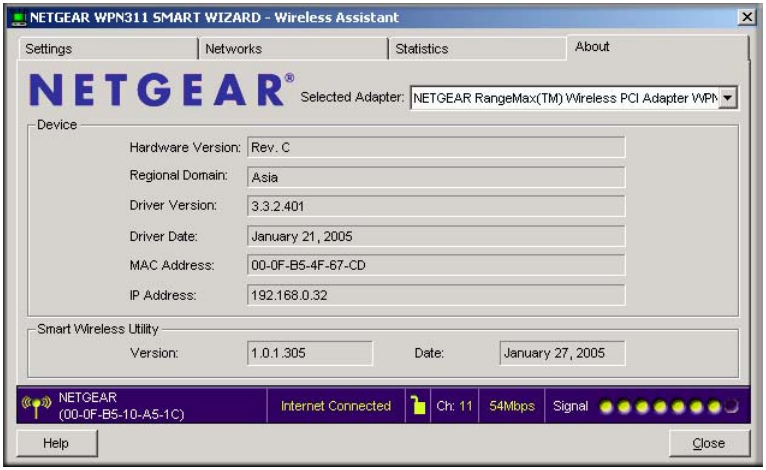


Figure 3-1: About page

The About page shows the following information:

- **Regional Domain:** This is the region setting for the wireless adapter. The approved channels for this region are automatically scanned. Governments regulate the channels used for wireless transmission. Operating the wireless adapter in a different region may violate local laws.
- **Driver Version:** The wireless adapter driver version.
- **Driver Date:** The wireless adapter driver release date.
- **MAC Address:** The MAC address of this adapter. The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Some wireless networks will restrict access based on a list of known MAC addresses. If you are communicating with such a network, you would have to provide the address shown here to the network administrator before you would be allowed to connect. Restricting access by MAC address adds an obstacle against unwanted access to your network. However, unless you use data encryption security, the data broadcast over the wireless link is fully exposed.
- **IP Address:** The IP address assigned to this adapter.
- **Configuration Utility Software:** The version and release date of this utility.

Chapter 4
Configuration

This section describes how to configure your NETGEAR RangeMax™ Wireless PCI Adapter WPN311 for wireless connectivity on your Wireless Local Area Network (WLAN) and use the data security encryption features.

Note: The instructions in this section refer to the NETGEAR WPN311 configuration utility. Windows XP users must first disable the Windows XP configuration utility. Open the network connections from the system tray icon, click the Properties button, click the Wireless Networks tab and then clear the "Use Windows to configure my wireless network settings" check box.

Understanding the Configuration Options

The WPN311 configuration utility provides a complete and easy to use set of tools to:

- Configure wireless settings.
- Monitor wireless network connections.
- Save your settings in configuration profiles.

The section below introduces these capabilities of the configuration utility.

Using Configuration Profiles

The WPN311 configuration utility uses profiles to store all the configuration settings for a particular wireless network. You can store multiple profiles and recall the one which matches the network you want to join.

For example, if you use your PC to connect to a wireless network in an office and a wireless network in your home, you can create a profile for each wireless network. Then, you can easily load the profile that has all the configuration settings you need to join the network you are using at the time.

There are two types of wireless network connections you can configure:

- **Infrastructure Mode —** uses the 802.11 infrastructure mode.
- **Ad-Hoc Mode** — uses the 802.11 ad-hoc mode

For more information on 802.11 wireless network modes, see "Wireless Networking Overview" on page B-1 of this manual.

Networks Page

The Networks page shows the available networks at your location.

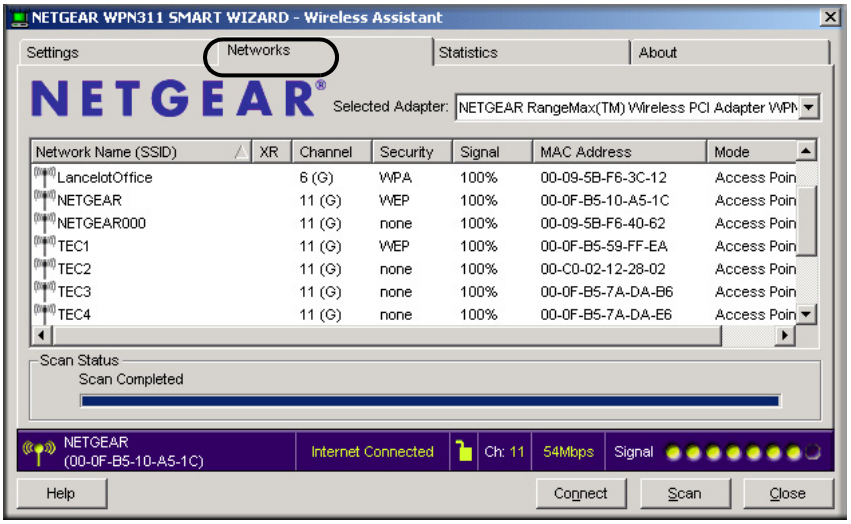


Figure 4-1: Networks tab page

The Networks page displays the following fields:

- **Wireless Network Name (SSID):** Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter. Note that, as a security measure, some wireless access points do not broadcast their SSID. In such cases, the SSID field will be blank even though the rest of the information will still be displayed.
- **Channel:** The channel determines which operating frequency will be used.
- **Security:** Identifies if the wireless network requires WEP or Advanced/WPA-PSK security settings.
- **Signal:** Identifies the signal strength of the communications.
- **MAC Address:** Identifies the hardware address (MAC Address) of the wireless device broadcasting this information.
- **Mode:** Identifies the type of wireless network — Access Point (Infrastructure) or Computer-to-computer (Ad-Hoc).

To connect to a network:

1. Click Scan to view the available networks.
2. Click on the column header to sort for better viewing if you have many networks.
3. Double-click to connect to the SSID.
4. The highlighted SSID is the one currently connected.

Connecting to an Access Point in Infrastructure Mode

This section provides instructions for configuring the NETGEAR RangeMax™ Wireless PCI Adapter WPN311 to connect to a wireless access point.

How to Configure an Infrastructure Mode Profile

Follow the instructions below to configure an infrastructure mode profile for connecting to an access point.

1. Run the WPN311 Configuration Utility.

a. Open the configuration utility by clicking on the WPN311 icon in the Windows system tray.

b. Click on the Settings tab to display the view shown below.

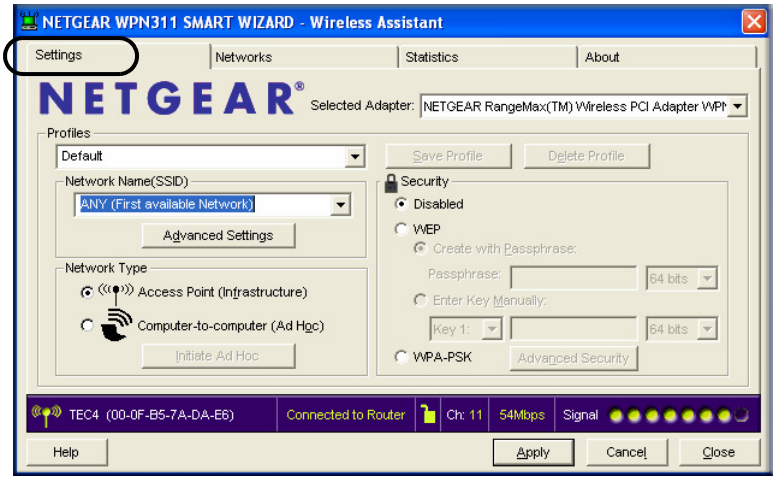


Figure 4-2: Settings tab page

2. Configure the wireless Network settings.

a. In the Network Type section, be sure that Infrastructure is selected.

b. Enter the SSID. This is also called the Wireless Network Name.

Note: You will not get a wireless network connection unless the network SSID matches exactly what is configured in the access point.

Tip: You can click the Networks tab to view a list of the available wireless networks and their SSIDs at your location.

3. Save your settings in a Profile.

a. Type a descriptive name for the Profile in the “Profiles” name field.

b. Click Save Profile. All the configuration settings are saved in this profile.

c. Click **Apply**.

d. Click Close to exit the configuration utility or Cancel to return to the previous settings.

4. Verify wireless connectivity to your network.

Verify connectivity by using a browser such as Netscape or Internet Explorer to connect to the Internet, or check for file and printer access on your network.

You can check the status bar in the configuration utility for the current connection status.

Note: If you cannot connect, see the "Basic Troubleshooting Tips" on page 3-12. Also, if you have problems accessing network resources, the Windows Client and File and Print Sharing software might not be installed and configured properly on your computers. Please refer to "Preparing Your Computers for TCP/IP Networking" on page C-1.

Connecting to Another PC in Ad-Hoc Mode

The computer-to-computer setting of the WPN311 uses Ad-Hoc mode. Ad-Hoc mode is an 802.11 networking framework in which devices or computers communicate directly with each other, without the use of an access point. For example, this mode is used when two Windows computers are configured with file and print sharing enabled and you want to exchange files directly between them.

How to Configure an Ad-Hoc Mode Profile

Note: Ad-Hoc mode will not work using DHCP settings. Ad-Hoc mode requires either static IP addresses (such as **`192.168.0.1)`** or other appropriate Windows networking configuration parameters such as adding IPX protocol support. For instructions on setting up static IP addresses or IPX protocol settings on a Windows PC, refer to the PC Networking Tutorial included on the *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD*.

Follow the instructions below to configure an Ad-Hoc mode profile.

1. **Run the WPN311 Configuration Utility.**

   a. Open the configuration utility by clicking on the WPN311 icon in the Windows system tray.

Figure 4-3: Settings tab page

b. Click the Settings tab to display the view shown above.

c. Select Ad-Hoc in the Network Type section.

d. Enter the SSID for the Ad-Hoc network.

e. Click **Apply**.

2. Save your settings in a Profile.

a. Type a descriptive name for the Profile Name.

b. Click Save Profile. All the configuration settings are saved in this profile.

c. Click **Apply**.

d. Click Close to exit the configuration utility.

3. Configure the PC network settings.

a. Configure each PC with either a static IP address or with the IPX protocol.

Note: For instructions on configuring static IP addresses or the IPX protocol, refer to the networking tutorial on your *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD*.

b. Restart the PCs.

4. Click Initiate Ad-Hoc.

The Ad-Hoc Setting dialog box will appear, as shown below.

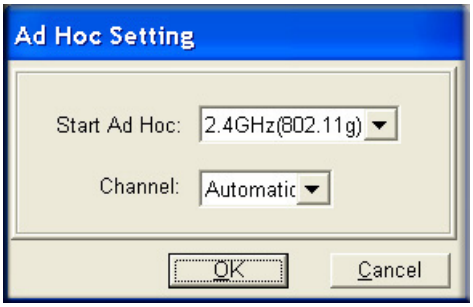


Figure 4-4: Ad-Hoc Setting page

a. The supported wireless standard is 802.11b/g for your Ad-Hoc computer-to-computer network.

b. In the Channel field, Automatic should work. If you notice interference problems with another nearby wireless device, select a channel that is not being used by any other wireless networks near your wireless adapter. Use the Networks tab page to identify the channels in use in your area.

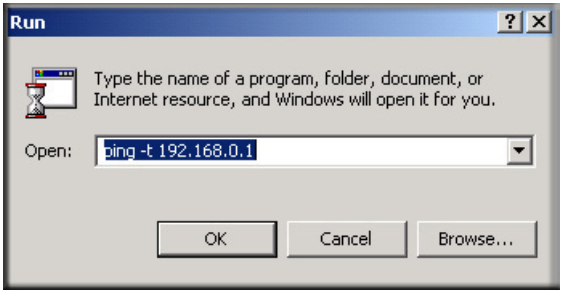
c. The channel number differs depending on the country. The connection speed automatically defaults to the highest speed.

d. Click **OK**.

5. Verify wireless connectivity between your peer devices.

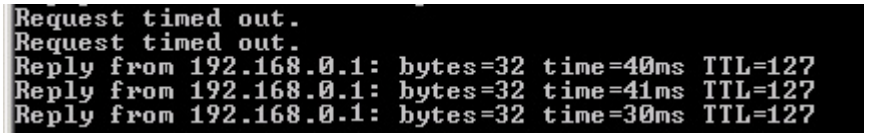
Verify connectivity by using the Ping program:

a. On the Windows taskbar click the Start button, and then click Run.



b. Assuming the target PC is configured with 192.168.0.1 as its IP address, type **`ping -t 192.168.0.1`** and then click OK.

c. This will cause a continuous ping to be sent to the device with the 192.168.0.1 static IP address. The ping response should change to "reply."


Request timed out.
Request timed out.
Reply from 192.168.0.1: bytes=32 time=40ms TTL=127
Reply from 192.168.0.1: bytes=32 time=41ms TTL=127
Reply from 192.168.0.1: bytes=32 time=30ms TTL=127

At this point the connection is established.

You may need to reboot in certain Windows operating systems such as Windows 98SE.

Note: If you cannot connect, see "Basic Troubleshooting Tips" on page 3-12. Also, if you have problems accessing network resources, the Windows Client and File and Print Sharing software might not be installed and configured properly on your computers. Please refer to "Preparing Your Computers for TCP/IP Networking" on page C-1.

Enabling Wireless Security Features

You can strengthen the security of your wireless connection by enabling encryption of the wireless data communications. This table summarizes the available security options of your NETGEAR RangeMax™ Wireless PCI Adapter WPN311.

Table 4-1. Wireless Security Options

Field	Description
WEP	WEP offers the following options: 64- or 128-bit WEP Data Encryption. Choose the Encryption Strength (64- or 128-bit data encryption). Manually enter the key values or enter a word or group of printable characters in the Passphrase box. Manually entered keys *are* case sensitive but passphrase characters *are not* case sensitive.
WPA-PSK	WPA-Pre-shared Key , uses 128-bit data encryption and dynamically changes the encryption keys making it nearly impossible to circumvent. Enter a word or group of printable characters in the Password Phrase box. These characters *are* case sensitive.

For more information on 802.11 wireless security, see Appendix B, "Wireless Networking Basics.

The procedures below identify how to configure the encryption settings of your NETGEAR RangeMax™ Wireless PCI Adapter WPN311.

Identifying the Wireless Security Settings

Print this form, fill in the configuration parameters and put it in a safe place for possible future reference. For an existing wireless network, the person who set up the network will be able to provide this information.

- ***Wireless Network Name (SSID):*** The Service Set Identification (SSID) identifies the wireless local area network. **ANY** is the default WPN311 wireless network name (SSID). You can customize it using up to 32 alphanumeric characters. Write your customized wireless network name (SSID) on the line below.

  Note: The SSID in the wireless access point is the SSID you configure in the wireless pc adapter. For the access point and wireless nodes to communicate with each other, all must be configured with the same SSID.

  Wireless network name (SSID): _____

- **If WEP Authentication is Used.**
  - **WEP Encryption key size**. Identify one: **64-bit** or **128-bit**. The encryption key size must the wireless network settings.
  - **Data Encryption (WEP) Keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces below.
    - **Passphrase method**. _____ These characters *are* case sensitive. Enter a word or group of printable characters and click the Generate Keys button. Not all wireless devices support the passphrase method.
    - **Manual method**. These values *are not* case sensitive. For 64-bit WEP, enter 10 hex digits (any combination of 0-9 or a-f). For 128-bit WEP, enter 26 hex digits.

    Key 1: _____

    Key 2: _____

    Key 3: _____

    Key 4: _____

- **If WPA-PSK Authentication is Used.**
  - **Passphrase**: _____ These characters *are* case sensitive. Enter a word or group of printable characters. When you use WPA-PSK, the other devices in the network will not connect unless they are set to WPA-PSK as well and are configured with the correct Passphrase.

Use the procedures below to configure basic security settings in the WPN311.

How to Configure WEP Encryption Security

Following the steps below to configure WEP Encryption Security.

1. **Run the WPN311 Configuration Utility.**

   a. Open the configuration utility by clicking on the WPN311 icon in the Windows system tray.

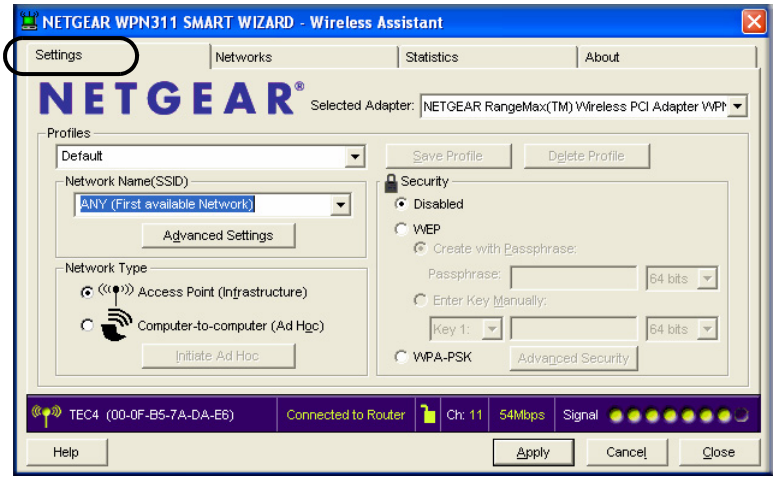


Figure 4-5: Settings tab page

   b. Click on the Settings tab to display the view shown above.

2. **Configure the Security settings.**

   a. Select the Use WEP Encryption check box.

   b. Enter the SSID. This is also called the Wireless Network Name.

      Note: You will not get a wireless network connection unless the network SSID matches exactly what is configured in the access point.

      Tip: You can click the Networks tab to view a list of the available wireless networks and their SSIDs at your location.

3. **Save your settings in a Profile.**

   a. Type a descriptive name for the Profile name.

   b. Click Save Profile. All the configuration settings are saved in this profile.

c. Click **Apply**.

d. Click Close to exit the configuration utility.

4. **Select the WEP encryption strength you will use.**

   The choices are:

   - 64-bit WEP data encryption
   - 128-bit WEP data encryption

   Note: Larger encryption keys require more processing and may slow the communications response times.

   a. Select Create with Passphrase and enter the passphrase. The configuration utility will automatically generate the WEP keys.

      Note: The characters are case sensitive. Be sure to use the same passphrase for all the wireless devices in the network.

      If the passphrase method is not available in the other devices, you must manually enter the keys to match exactly what is in the access point and other 802.11 wireless devices.

   b. The Default Key setting must match what is set in the access point and the other 802.11 wireless devices.

5. **Click Apply for the changes to take effect.**

How to Configure WPA-PSK Encryption Security

Wi-Fi Protected Access (WPA) is wireless security with far greater protection than WEP. WPA-PSK (pre-shared key) uses encryption of a shared key as the starting point. WPA has a significant advantages over WEP — an encryption key differing in every packet. It is extremely difficult for hackers to read messages even if they have intercepted the data.

To configure WPA-PSK security, click the Advanced Security button. The Advanced Security button is located in the Settings page, Security section.

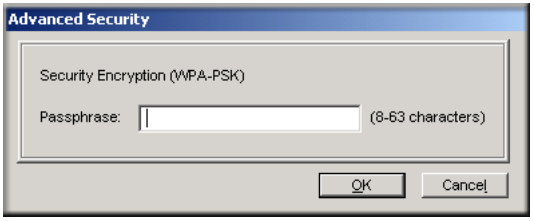


Figure 4-6: Advanced Security page

The Passphrase can be between 8 and 63 characters

For more information on WPA security, see "WPA Wireless Security" on page B-8.

Statistics Page

The Statistics page provides real time and historical trend information on the data traffic and performance of your wireless adapter.

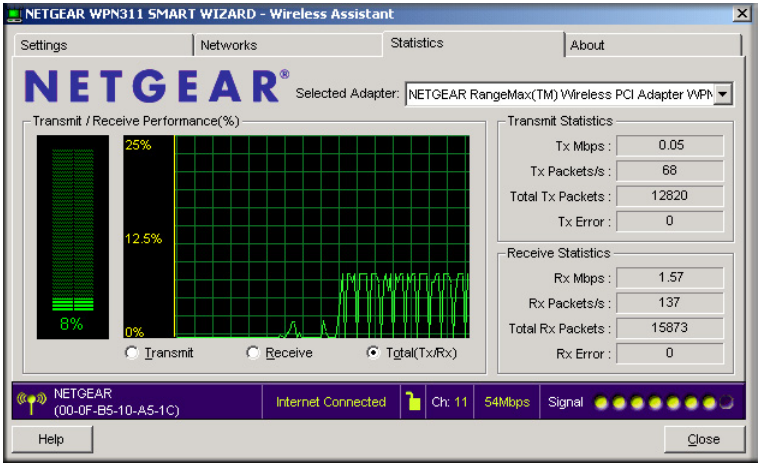


Figure 4-7: Statistics tab page

- **Transmit/Receive Performance (%):** A real time graph identifying the transmit, receive, or total utilization as a percentage the total possible. The Transmit, Receive, and Total (TxRx) radio buttons let you select whether to display the transmit performance, the receive performance, or the total of both in the same graph. Total is the default.
- **Transmit Statistics:** Identifies Transmit megabits per second (Mbps), transmit packets per second (Tx Packets/s), total transmitted packets, and transmit errors.
- **Receive Statistics:** Identifies Receive megabits per second (Mbps), receive packets per second (Rx Packets/s), total received packets, and received errors.

Advanced Settings Page

Generally, the Advanced settings should not require adjustment. Except for the power saving setting, changing any of the settings incorrectly on this page could cause your wireless connection to fail.To display the Advanced Settings Page, click the Advanced Settings button on the Settings Page.

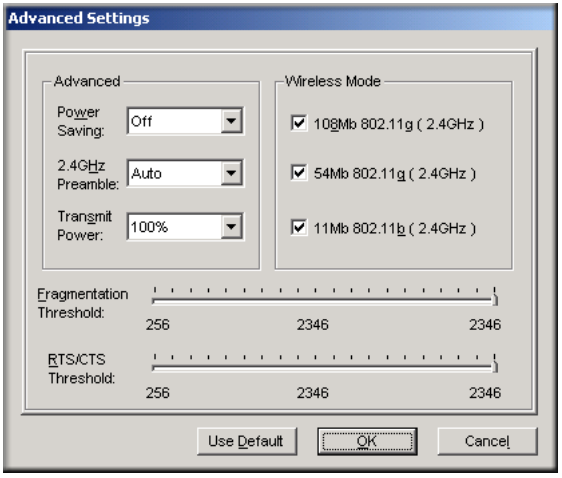


Figure 4-8: Advanced Settings page

- **Power Saving:** Select On if you are using a notebook computer running on battery power.
- **Preamble:** A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble might give slightly better performance.

- **Transmit Power:** Lowering the output power level lets you reduce the chance of interference with other nearby access points but reduces the range of your adapter.
- **Wireless Mode:** Select the wireless protocols you will use. Depending on your wireless adapter, you can choose some or all of the available 802.11 wireless protocols. Note that, if the wireless network you are communicating with uses the 108Mb Turbo mode, you must include that in your selection.
- **Fragmentation Threshold:** This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.
- **RTS/CTS Threshold:** RTS is request to send and CTS is clear to send; their purpose is to avoid collisions. RTS/CTS will be enabled if the data frame size is larger than the threshold value set here. The maximum frame size is 2346 octets, so if the threshold is 2346, RTS/CTS will be disabled.

  Note: This setting is reserved for wireless testing and advanced configuration only. Do not change this setting unless you are sure you need to. The primary reason for implementing RTS/CTS is to minimize collisions between hidden stations. This occurs when users and access points are spread out and a high number of retransmissions occur on the wireless LAN.

Chapter 5
Troubleshooting

This chapter provides information about troubleshooting your NETGEAR RangeMax™ Wireless PCI Adapter WPN311. After each problem description, instructions are given to help you diagnose and solve the problem.

Also, for problems with accessing network resources, the Windows software might not be installed and configured properly on your computers. Please refer to Appendix C, "Preparing Your PCs for Network Access" of the Reference Manual on the *NETGEAR RangeMax™ Wireless PCI Adapter WPN311 Resource CD*.

Frequently Asked Questions

Use the information below to solve common problems you may encounter. Also, please refer to the knowledge base on the NETGEAR Web site at *www.netgear.com/support/main.asp*.

General Questions

Why do I see no more than 54 Mbps on the Configuration Utility status line?

The product literature says the WPN311 can operate at 108 Mbps. You are probably connecting to a standard 802.11g network. If you use the NETGEAR WGT624 108 Mbps Wireless Firewall Router or WG634U 108 Mbps Wireless Media Router, you will see network speeds up to 108 Mbps.

The WPN311 Smart Configuration Utility keeps asking me to save my settings

This is because you have made changes to the settings and the utility is offering you the chance to save the changes. If you want to avoid these Profile setting prompts, simply click Apply before you close the utility program.

Ad Hoc mode is not working correctly

You need to click the Initiate Ad Hoc button before you click Apply. Here is how you start an Ad Hoc network:

1. Fill in the Network Name (SSID).
2. Select the Computer-to-Computer (Ad Hoc) Network Type.
3. Click Initiate Ad Hoc.
4. Accept the default settings or make your changes and click OK
5. Click **Apply**.

Note: Be sure all computers in your Ad Hoc network are configured with static IP addresses in the same subnet.

How to know if the WPN311 card has received a valid IP address from the Wireless Router/AP

The easiest way is to open up the WPN311 utility program and check the IP address in the About page.

How to use XP's own Wireless configuration utility that comes with Windows XP

The NETGEAR WPN311 software is designed so that the user will be asked to choose one of the utility programs during initial software installation. Be sure the WPN311 is connected to the PC and follow these instructions to change your selection.

1. Go to Control Panel and select Network Connections.
2. Right click on the connection and select Properties.
3. Click the Wireless Networks tab.
4. Select or clear the WPN311 "Use Windows to configure my wireless network settings" check box.

How to remove the WPN311 utility and software

To remove the WPN311 software, go to Windows Start > Programs > NETGEAR WPN311 Smart Wizard. Select Uninstall NETGEAR WPN311 software.

I cannot connect to the AP that I want from the Networks browser list

The access point is available and there is good signal strength. There are a few possibilities:

- If the access point (AP) is WPA-PSK protected, you will need to have the correct WPA-PSK passphrase. Otherwise, the WPN311 will still be connected to the previous access point and you will not be able to change to the WPA-PSK access point.
- If the access point is WEP protected (either 64 or 128 bit encryption), you will be prompted to enter the WEP encryption security information.

The WPN311 is not getting an IP address

You probably upgraded your WPN311 software and did not reboot your system.

To get an IP address assigned, you can either restart your computer or choose another access point to connect to. If there are no additional access points for you to choose from, restart your system and connect to your desired access point again.

Note: It does not usually help to shut down the utility or disable/enable the card.

Wi-Fi Protected Access (WPA) Questions

Why is my WPN311 not connecting to my WPA router?

I thought I chose my WPA router in XP Zero Configuration's Available networks and it is showing other devices in the Preferred networks list, why is my WPN311 not connecting to my WPA router?

Check your Preferred networks and remove the other non-WPA devices from the list. Only leave your WPA router in the list and try connecting again.

Why is the icon in the System Tray flashing Green to Red alternately?

I thought I got my WPN311 WPA connection – a green icon in the SystemTray.

Although you have use XP zero configuration utility for your WPA settings, the open "Green-Red" flashing icon indicates that you might have entered the incorrect WPA secret key. Assure that the WPA settings are configured correctly on both the Radius Server and the Router. In addition, you may also check the Radius' port number on the Radius server and the router.

How do I know that my WPN311 WPA is working?

Try browsing an Internet site to see if your WPA router has an Internet connection. Or try pinging the Radius server through the WPA router.

Why is the WAN port not working after configuring WPA?

I can ping the WPA router but there is no Internet connection. I know that the WAN port was not working before my WPA connection.

One thing to check is the DHCP on the WPA router. Make sure the DHCP server or DHCP client option is correctly set. You may also check the Radius server's DHCP settings.

Note: For all WPA questions, please refer to Microsoft's Help documentation for additional WPA related information and how to configure WPA using Windows XP Zero configuration utility.

Appendix A
Technical Specifications

This appendix provides technical specifications for the NETGEAR RangeMax™ Wireless PCI Adapter WPN311.

Antennae	Detachable antenna
Radio Data Rate	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps (Auto Rate Sensing)
Frequency	2.4GHz to 2.5GHz CCK and OFDM Modulation)
Emissions	FCC, CE
Bus interface	PCI
Provided drivers	Microsoft Windows 98SE, 2000, Me, XP
Weight	40 g
LED	Power, Activity
Operating Environment	Operating temperature: 0 to 55 degrees C, 32 to 131 degrees F
Encryption	40-bit (also called 64-bit) and 128-bit WEP data encryption

Appendix B
Wireless Networking Basics

This chapter provides an overview of Wireless networking.

Wireless Networking Overview

The WPN311 Wireless PCI Adapter conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b and 802.11 g standards for wireless LANs (WLANs)WPN311. On an 802.11b or g wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.4GHz. The maximum data rate for the wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected. The 802.11g auto rate sensing rates are 1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network - Ad-Hoc and infrastructure.

Infrastructure Mode

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless network connection.

Ad-Hoc Mode (Peer-to-Peer Workgroup)

In an ad-hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no Access Point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft networking in the various Windows operating systems. Some vendors also refer to ad-hoc networking as peer-to-peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Network Name: Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad-hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

Authentication and WEP

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

802.11 Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 Station can communicate with an Ethernet network through an access point such as the one built in to the WPN311:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available Access Point within range, regardless of its SSID.
- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

Open System Authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.
2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

This process is illustrated in below.

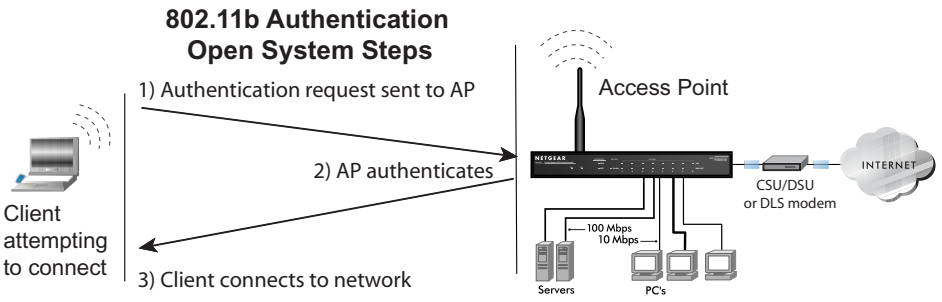


Figure 5-1: 802.11 open system authentication

Shared Key Authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (i.e., the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

This process is illustrated in below.

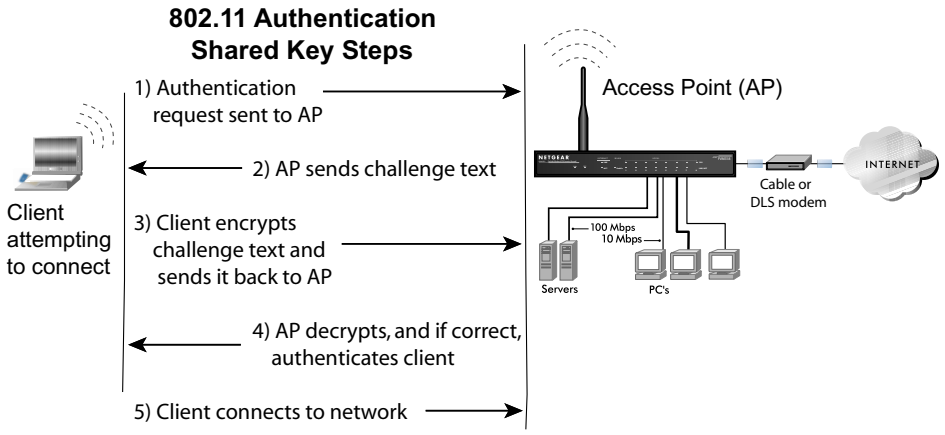


Figure 5-2: 802.11 shared key authentication

Overview of WEP Parameters

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.

2. **Use WEP for Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11 device decrypts the data using the same WEP Key. For authentication purposes, the 802.11 network uses Open System Authentication.

3. **Use WEP for Authentication and Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11 device decrypts the data using the same WEP Key. For authentication purposes, the 802.11 network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption).

Key Size

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP Keys. Each 40-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP Key.

When configured for 128-bit encryption, 802.11 products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP Key.

Note: Typically, 802.11 access points can store up to four 128-bit WEP Keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters configurations match.

WEP Configuration Options

The WEP settings must match on all 802.11 devices that are within the same wireless network as identified by the SSID. In general, if your mobile clients will roam between access points, then all of the 802.11 access points and all of the 802.11 client adapters on the network must have the same WEP settings.

Note: Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

Note: The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

Wireless Channels

IEEE 802.11b and g wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used are listed in Table 5-1:

Table 5-1. 802.11b and g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Note: The available channels supported by the wireless products in various countries are different.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

WPA Wireless Security

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

The IEEE introduced the WEP as an optional security measure to secure 802.11b (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious. In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the shortcomings of WEP. This standard, formerly known as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture being defined in the IEEE.

WPA offers the following benefits:

- Enhanced data privacy
- Robust key management
- Data origin authentication
- Data integrity protection

The Wi-Fi Alliance is now performing interoperability certification testing on Wi-Fi Protected Access products. Starting August of 2003, all new Wi-Fi certified products will have to support WPA. NETGEAR will implement WPA on client and access point products and make this available in the second half of 2003. Existing Wi-Fi certified products will have one year to add WPA support or they will lose their Wi-Fi certification.

The 802.11i standard is currently in draft form, with ratification due at the end of 2003. While the new IEEE 802.11i standard is being ratified, wireless vendors have agreed on WPA as an interoperable interim standard.

How Does WPA Compare to WEP?

WEP is a data encryption method and is not intended as a user authentication mechanism. WPA user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Support for 802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional. For details on EAP specifically, refer to IETF's RFC 2284.

With 802.11 WEP, all access points and client wireless adapters on a particular wireless LAN must use the same encryption key. A major problem with the 802.11 standard is that the keys are cumbersome to change. If you do not update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. Products based on the 802.11 standard alone offer system administrators no effective method to update the keys.

For 802.11, WEP encryption is optional. For WPA, encryption using Temporal Key Integrity Protocol (TKIP) is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of the known WEP vulnerabilities.

How Does WPA Compare to IEEE 802.11i?

WPA will be forward compatible with the IEEE 802.11i security specification currently under development. WPA is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that are ready to bring to market today, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in WPA are secure IBSS (Ad Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols, such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

What are the Key Features of WPA Security?

The following security features are included in the WPA standard:

- WPA Authentication
- WPA Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael message integrity code (MIC)
  - AES Support (to be phased in)
- Support for a Mixture of WPA and WEP Wireless Clients, but mixing WEP and WPA is discouraged

These features are discussed below.

WPA addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (for example, user names and passwords) and authenticates wireless users before they gain access to the network.

The strength of WPA comes from an integrated sequence of operations that encompass 802.1X/ EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- Network security capability determination. This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).

  The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured pass phrase on both the stations and the access point. This obviates the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible cipher suites include: WEP, TKIP, and AES (Advanced Encryption Standard). We talk more about TKIP and AES when addressing data privacy below.

- Authentication. EAP over 802.1X is used for authentication. Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. 802.1X port access control prevents full access to the network until authentication completes. 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

  The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

- Key management. WPA features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent 4-way handshake between the station and Access Point (AP).

- Data Privacy (Encryption). Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.

- Data integrity. TKIP includes a message integrity code (MIC) at the end of each plaintext message to ensure messages are not being spoofed.

WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

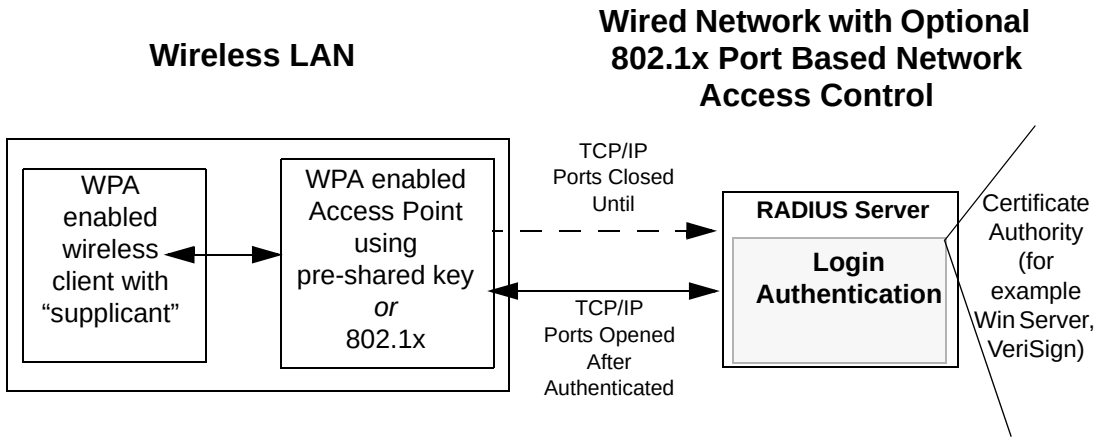

Wireless LAN
Wired Network with Optional 802.1x Port Based Network Access Control
WPA enabled wireless client with "supplicant"
WPA enabled Access Point using pre-shared key or 802.1x
TCP/IP Ports Closed Until
TCP/IP Ports Opened After Authenticated
RADIUS Server
Login Authentication
Certificate Authority (for example Win Server, VeriSign)

Figure B-1: WPA Overview

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as providing a vehicle for dynamically varying data encryption keys via EAP from a RADIUS server, for example. This framework enables using a central authentication server, which employs mutual authentication so that a rogue wireless user does not join the network.

It is important to note that 802.1x does not provide the actual authentication mechanisms. When using 802.1x, the EAP type, such as Transport Layer Security (EAP-TLS), or EAP Tunneled Transport Layer Security (EAP-TTLS), defines how the authentication takes place.

Note: For environments with a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a pre-shared key.

Together, these technologies provide a framework for strong user authentication.

Windows XP implements 802.1x natively, and several NETGEAR switch and wireless access point products support 802.1x.

Client with a WPA-enabled wireless adapter and supplicant (Win XP, Funk, Meetinghouse)

For example, a WPA-enabled AP

For example, a RADIUS server

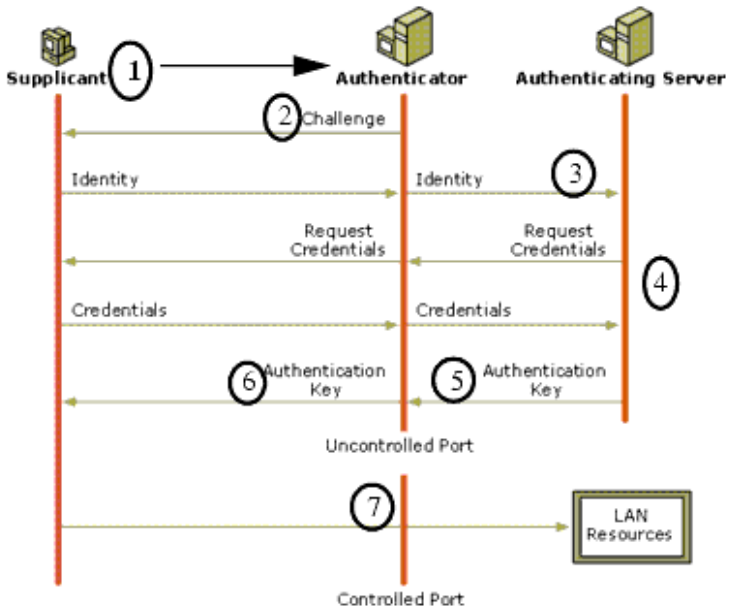


Figure B-2: 802.1x Authentication Sequence

The AP sends Beacon Frames with WPA information element to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

1. Initial 802.1x communications begin with an unauthenticated supplicant (client device) attempting to connect with an authenticator (802.11 access point). The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.

3. The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (for example, RADIUS).
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application “supplicant” software on the client devices. The access point acts as a “pass through” for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant access point. As a result, you can update the EAP authentication type to such devices as token cards (Smart Cards), Kerberos, one-time passwords, certificates, and public key authentication, or as newer types become available and your requirements for security change.

WPA Data Encryption Key Management

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required.

For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility (the Information Element) for the wireless AP to advertise the changed key to the connected wireless clients.

If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

Temporal Key Integrity Protocol (TKIP)

WPA uses TKIP to provide important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

Michael

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte *message integrity check* (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

Optional AES Support to be Phased In

One of the encryption methods supported by WPA, besides TKIP, is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but the problem with AES is that it requires a fundamental redesign of the NIC's hardware in both the station and the access point. TKIP is a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

Is WPA Perfect?

WPA is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the message integrity code (MIC) within 60 seconds of each other, then the network is under an active attack, and as a result, the access point employs counter measures, which include disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds. More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

Product Support for WPA

Starting in August, 2003, NETGEAR, Inc. wireless Wi-Fi certified products will support the WPA standard. NETGEAR, Inc. wireless products that had their Wi-Fi certification approved before August, 2003 will have one year to add WPA so as to maintain their Wi-Fi certification.

WPA requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

Supporting a Mixture of WPA and WEP Wireless Clients is Discouraged

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

However, a mixed mode supporting WPA and non-WPA clients would offer network security that is no better than that obtained with a non-WPA network, and thus this mode of operation is discouraged.

Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA information element**
  To advertise their support of WPA, wireless APs send the beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless access points to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless AP.

Changes to Wireless Network Adapters

Wireless networking software in the adapter, and possibly in the OS or client application, must be updated to support the following:

- **The new WPA information element**
  Wireless clients must be able to process the WPA information element and respond with a specific security configuration.
- **The WPA two-phase authentication**
  Open system, then 802.1x supplicant (EAP or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless network adapters to support WPA, obtain a WPA update from your wireless network adapter vendor and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update in the wireless adapter driver. So, to update your Microsoft Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA authentication (and preshared key) and the new WPA encryption algorithms (TKIP and the optional AES component).

To obtain the Microsoft WPA client program, visit the Microsoft Web site.

Appendix C
Preparing Your PCs for Network Access

This appendix describes how to prepare your PCs to connect to the Internet through the NETGEAR RangeMax™ Wireless PCI Adapter WPN311.

For adding file and print sharing to your network, please consult the Windows help information included with the version of Windows installed on each computer on your network.

Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/ IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP. Windows 95 or later includes the software components for establishing a TCP/IP network.

In your TCP/IP network, each PC and the wireless access point must be assigned a unique IP addresses. Each PC must also have certain other TCP/IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during startup.

Configuring Windows 98SE and Me for TCP/IP Networking

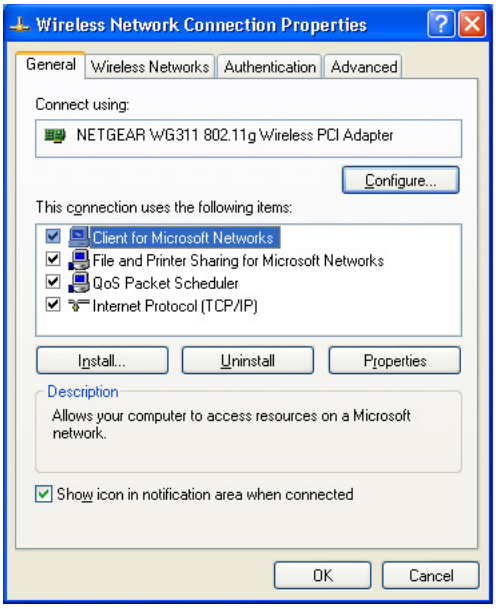
As part of the PC preparation process, you may need to install and configure TCP/IP on your PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:



   You must have an Ethernet adapter or an WPN311, the TCP/IP protocol, and the Client for Microsoft Networks.

   If you need to add TCP/IP:

   a. Click the Add button.
   b. Select Protocol, and then click Add.
   c. Select Microsoft.
   d. Select TCP/IP, and then click OK.

   If you need to add the Client for Microsoft Networks:

   a. Click the Add button.
   b. Select Client, and then click Add.
   c. Select Microsoft.

d. Select Client for Microsoft Networks, and then click OK.

If you need to add File and Print Sharing for Microsoft Networks:

a. Click the Add button.
b. Select Client, and then click Add.
c. Select Microsoft.
d. Select File and Print Sharing for Microsoft Networks, and then click OK.

3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 98SE and Me

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

Locate your **Network Neighborhood** icon.

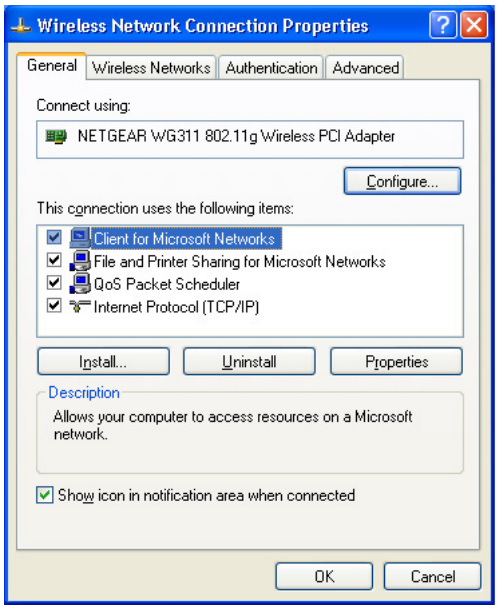
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
  - Click **Start** on the task bar located at the bottom left of the window.
  - Choose **Settings**, and then **Control Panel**.
  - Locate the **Network Neighborhood** icon and click on it. This will open the Network panel as shown below.

2

Verify the following settings as shown:

- Client for Microsoft Network exists
- Ethernet adapter is present
- TCP/IP is present
- **Primary Network Logon** is set to Windows logon

Click on the **Properties** button. The following TCP/IP Properties window will display.



3

By default, the **IP Address** tab is open on this window.

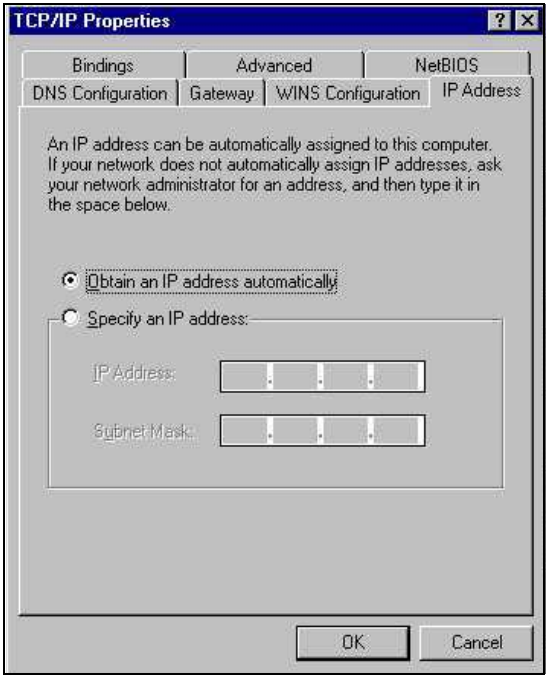
- Verify the following:

  Obtain an IP address automatically is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.

- Click **OK** to continue.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Selecting the Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select “I want to set up my Internet connection manually” or “I want to connect through a Local Area Network” and click Next.
4. Select “I want to connect through a Local Area Network” and click Next.
5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.

2. Type **winipcfg**, and then click OK.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

Configuring Windows 2000 or XP for TCP/IP Networking

As part of the PC preparation process, you may need to install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dial-up Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.
5. Verify that ‘Client for Microsoft Networks’ and ‘Internet Protocol (TCP/IP)’ are present. If not, select Install and add them.
6. Select ‘Internet Protocol (TCP/IP)’, click Properties, and verify that “Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dial-up Connections windows.
8. Then, restart your PC.

DHCP Configuration of TCP/IP in Windows XP or 2000

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

DHCP Configuration of TCP/IP in Windows XP

1

Locate your **Network Neighborhood** icon.

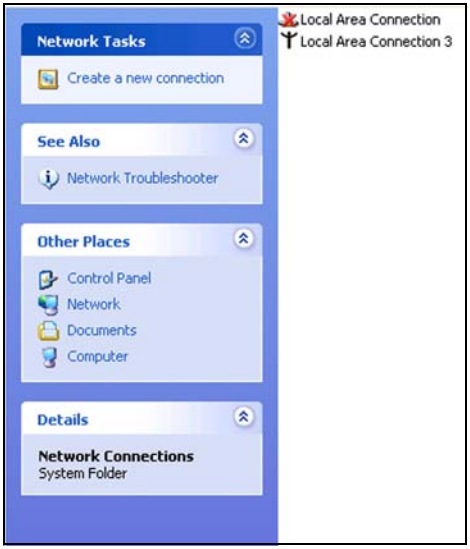
- Select **Control Panel** from the Windows XP Start Menu.
- Select the **Network Connections** icon on the Control Panel. This will take you to the next step.

2

Now the Network Connection window displays.

The Connections List that shows all the network connections set up on the PC, located to the right of the window.

- Right-click on the **Connection with the wireless icon** and choose **Status**.



3

Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.

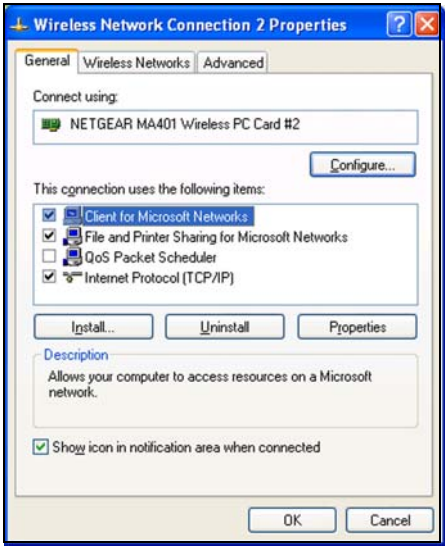
Administrator logon access rights are needed to use this window.

- Click the **Properties button** to view details about the connection.

4

The TCP/IP details are presented on the Support tab page.

- Select **Internet Protocol,** and click **Properties** to view the configuration information**.**



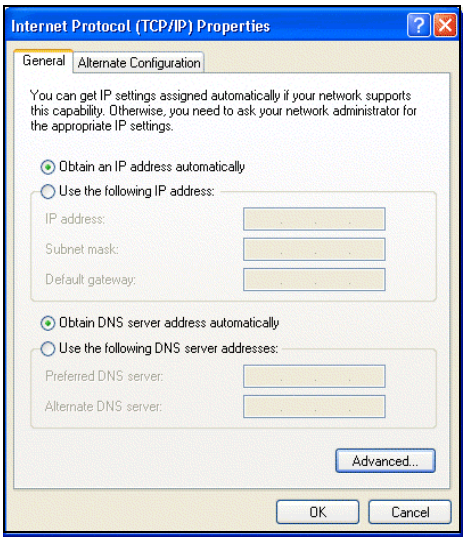
5

Verify that **Obtain an IP address automatically** radio button is selected and that the **Obtain DNS server address automatically** radio button is selected.

• Click the **OK** button.

This completes the DHCP configuration in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

DHCP Configuration of TCP/IP in Windows 2000

After you install a network card, TCP/IP for Windows 2000 is configured and set to DHCP without your having to configure it. However, if there are problems, following the steps below to configure TCP/IP with DHCP for Windows 2000.

1

Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.

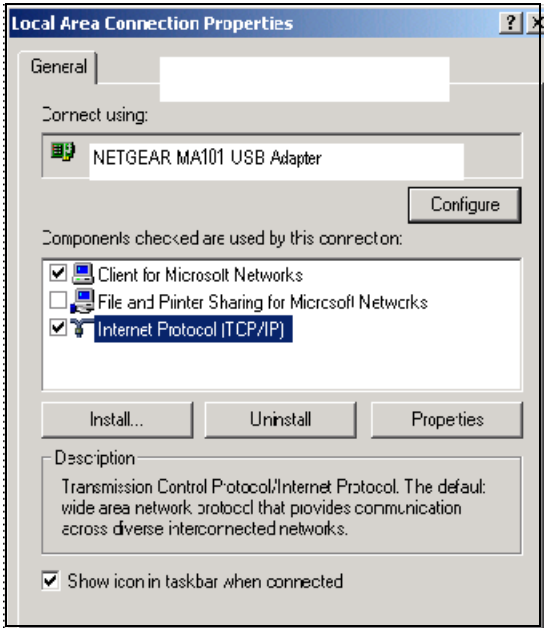
• Right click on **Local Area Connection** and select **Properties**.

2

The **Local Area Connection Properties** dialog box appears. Verify that you have the correct Ethernet card selected in the **Connect using:** box and that the following two items are displayed and selected in the box of "Components checked are used by this connection:"

- Client for Microsoft Networks and
- Internet Protocol (TCP/IP)

Click **OK**.


Local Area Connection Properties
General
Connect using:
NETGEAR MA101 USB Adapter
Configure
Components checked are used by this connection:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in taskbar when connected

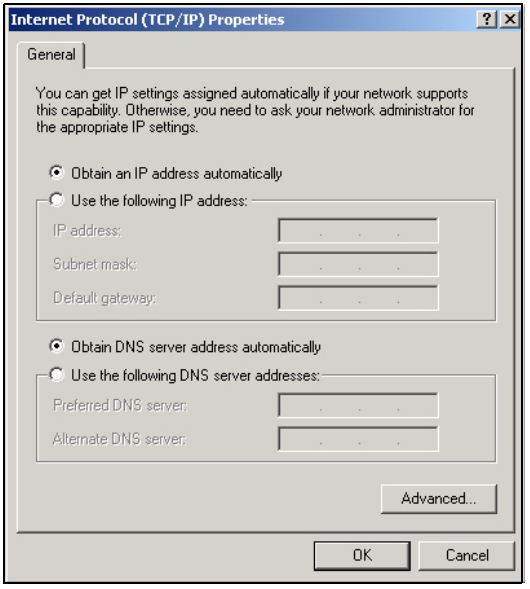
3

With Internet Protocol (TCP/IP) selected, click on **Properties** to open the Internet Protocol (TCP/IP) Properties dialogue box. Verify that

- **Obtain an IP address automatically** is selected.
- **Obtain DNS server address automatically** is selected.

Click **OK** to return to Local Area Connection Properties. Click **OK** again to complete the configuration process.

Restart the PC. Repeat these steps for each PC with this version of Windows on your network.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Verifying TCP/IP Properties for Windows XP or 2000

To check your PC's TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

   The Run window opens.

2. Type **cmd** and then click OK.

   A command window opens

3. Type **ipconfig /all**

   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

4. Type **exit**

Glossary

List of Glossary Terms

Use the list below to find definitions for technical terms used in this manual.

10BASE-T
IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx
IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.11b
IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz.

802.11g
An IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz. 802.11g is backwards compatible with 802.11b.

ADSL
Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DHCP
An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

DNS
Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.
Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to

198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name
A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DSL
Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

Dynamic Host Configuration Protocol
DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

ESSID
The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

Gateway
A local device, usually a router, that connects hosts on a local network to other networks.

IETF
Internet Engineering Task Force. Working groups of the IETF propose standard protocols and procedures for the Internet, which are published as RFCs (Request for Comment) at *www.ietf.org*.
An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IP
Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address
A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
Ranges of addresses are assigned by Internic, an organization formed for this purpose.

IPX
Short for Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems.
Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services.

ISP
Internet service provider.

Internet Protocol
The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

LAN
A communications network serving users within a limited area, such as one floor of a building.

local area network
LAN. A communications network serving users within a limited area, such as one floor of a building.
A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.

MAC address
The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Mbps
Megabits per second.

NetBIOS
The Network Basic Input Output System is an application programming interface (API) for sharing services and information on local-area networks (LANs).
Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, up to 16 characters in length.

Network Address Translation
NAT. A technique by which several hosts share a single IP address for access to the Internet.

NIC
Network Interface Card. An adapter in a computer which provides connectivity to a network.

packet
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

Routing Information Protocol
RIP. A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

SSID
A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.
This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

Subnet Mask
A mask used to determine what subnet an IP address belongs to. Subnetting enables a network administrator to further divide an IP address into two or more subnets.

TCP/IP
The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

WAN
A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

WEB Proxy Server
A Web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall.
The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

WEP
Wired Equivalent Privacy is a data encryption protocol for 802.11 wireless networks.
All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.

wide area network
WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

Wi-Fi
A trade name for the 802.11 wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11 devices.

Windows Internet Naming Service
WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.
If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS
WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Wireless Network Name (SSID)
Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

WPA
Wi-Fi Protected Access (WPA) is data encryption protocol for 802.11 wireless networks. With WPA-PSK (pre-shared key), all wireless nodes and access points on the network are configured with a Shared Key for data encryption.

Index

Numerics

802.11b 1

A

Ad-Hoc Mode 2
ad-hoc mode 2
Ad-Hoc Mode Profile 5

B

BSSID 2

C

Configuration Profiles 1

E

ESSID 2

F

features 1

I

Infrastructure Mode 2
infrastructure mode 2
Infrastructure Mode Profile 3
IP networking
  for Windows 1, 6

N

Networks Page 2

O

Open System authentication 2

P

Passphrase 8, 9
Profiles 1

S

Shared Key authentication 2
SSID 3, 2

T

TCP/IP properties
  verifying for Windows 5
troubleshooting 1

W

WEP 4, 2
Wi-Fi 1
Wi-Fi Protected Access (WPA) 11
Windows, configuring for IP routing 1, 6
winipcfg utility 5
Wired Equivalent Privacy. *See* WEP
Wireless Ethernet 1
wireless network name 3
WPA 11
WPA-PSK 8
WPA-PSK Password Phrase 8